D/F

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

-against-

FABIO GASPERINI,

Defendant.

MEMORANDUM & ORDER

16-CR-441 (NGG)

----------X
NICHOLAS G. GARAUFIS, United States District Judge.

Defendant Fabio Gasperini ("Defendant") is charged with two counts of computer intrusion, one count of conspiracy to commit wire fraud, one count of wire fraud, and one count of conspiracy to commit money laundering. (See Indictment ("Ind.") (Dkt. 3) ¶¶ 11-21.) The charges stem from Defendant's alleged creation of a "botnet" to further a "click fraud" perpetrated against advertising companies. (Id. ¶¶ 1-10.) The Government alleges that Defendant and others obtained unauthorized access to computers in the U.S. and around the world and remotely directed those computers to fraudulently inflate the number of times that online advertisements were "viewed."

Currently pending before the court are Defendant's motion to dismiss the indictment (Mot. to Dismiss ("MTD") (Dkt. 9)), motion for a bill of particulars (Mot. for Bill of Particulars ("BOP Mot.") (Dkt. 36)), and motion for disclosure of grand jury materials (Mot. for Grand Jury Tr. ("GJ Mot.") (Dkt. 35)). For the following reasons, Defendant's motions to dismiss and for disclosure of grand jury materials are DENIED and his motion for a bill of particulars is GRANTED IN PART and DENIED IN PART.

I. BACKGROUND

A. Allegations

The following statement of facts is drawn from the Indictment, the Complaint, and an Affidavit submitted in connection with Defendant's extradition to the United States.

Defendant is an Italian national who resided in Rome at all relevant times. (Ind. ¶ 1.) The Government's primary allegation is that Defendant engaged in "click fraud," a scheme in which an individual:

1) enters into a contract with an advertising company in which the individual (a) places online advertisements onto a websites and (b) receives compensation from the company based on the number of times that users "click" on their ads, and then

2) places malicious software ("malware") onto one or more third-party computers and servers that directs those computers to click on their advertisements and artificially drives up the number of "clicks" for which the individual is compensated.

(See id. ¶¶ 1-4.) In connection with these schemes, individuals may develop a "botnet," defined by the Indictment as "a network of computers, such as servers, infected with malicious software without the users' knowledge or authorization." (Id. ¶ 1.) The botnet's creator can then remotely direct the network of compromised computers to engage in coordinated action and, in a "click fraud" scheme, can "remotely command a botnet to flood a particular website advertisement with electronic communications that register with the advertising company as clicks by a human user." (Id. ¶ 4.)

The Indictment alleges that between February 2011 and June 2016, Defendant and others "surreptitiously gained entry into multiple computer servers . . . in the United States and elsewhere" without authorization (id. ¶ 6) and "installed . . . malicious software," creating a

botnet (id. ¶ 7). The Indictment alleges that, "[i]n establishing this botnet, [Defendant] also obtained unauthorized access to sensitive data and files stored on the compromised servers." (Id.) Defendant allegedly used the botnet to commit "click fraud" against various businesses and advertising companies, including one named Italian advertising company. (Ex. A. to Opp'n to MTD ("Extradition Aff.") (Dkt. 27-1) ¶ 10.) The Indictment further alleges that Defendant laundered proceeds from the alleged "click fraud" through other individuals "in order to conceal the nature of the payments and his identity." (Ind.¶ 10.)

B. Procedural History

Defendant was arrested in Amsterdam in June 18, 2016, and extradited to the United States on April 20, 2017. (Opp'n to MTD ("MTD Opp'n") (Dkt. 27) at 2.) On August 4, 2016, a federal grand jury returned an Indictment charging Defendant with two counts of computer intrusion (the "Computer Intrusion Counts"), wire fraud and conspiracy to commit wire fraud (the "Wire Fraud Counts"); and conspiracy to launder money. (Ind. ¶¶ 11-21.)

On April 24, 2017, Defendant moved to dismiss the Indictment. (See MTD). Defendant subsequently moved for both a bill of particulars and for disclosure of grand jury material. (See BOP Mot.; GJ Mot.)

II. DISCUSSION

A. Motion to Dismiss the Indictment

Defendant's motion to dismiss asserts three primary arguments: (1) the Computer Intrusion Counts under 18 U.S.C. §§ 1030(a)(2) and 1034(a)(4) are insufficiently pled; (2) the statutes underlying the Wire Fraud Counts cannot be applied extraterritorially; and (3) application of the Wire Fraud and Computer Intrusion Counts to Defendant would violate his due process rights. (MTD at 2.) The court disagrees with Defendant on each of these points and accordingly denies Defendant's motion to dismiss.

1. Legal Standard

"[An] indictment . . . must be a plain, concise, and definite written statement of the essential facts constituting the offense charged . . . ." Fed. R. Crim. P. 7(c). "[A]n indictment is sufficient if it, first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an acquittal or convictions in bar of future prosecutions for the same offense." United States v. Alfonso, 143 F.3d 772, 776 (2d Cir. 1998) (quoting Hamling v. United States, 418 U.S. 87, 117 (1974)). This generally requires an Indictment to "do little more than [] track the language of the statute charged and state the place and time (in approximate terms) of the alleged crime." United States v. Walsh, 194 F.3d 37, 44 (2d Cir. 1999) (internal quotation marks and citations omitted).

Defendants may raise pretrial challenges to the sufficiency and specificity of an indictment "if the basis for the motion is reasonably available and the motion can be determined without a trial on the merits." See Fed. R. Crim. P. 12(b)(3)(B)(iii), (v). "[I]n deciding a pretrial motion to dismiss, the Court must accept the Government's factual allegations as true," United States v. Carnesi, 461 F. Supp. 2d 97, 98 (E.D.N.Y. 2006), and the "indictment must be read to include facts which are necessarily implied by the specific allegations made," United States v. Stavroulakis, 952 F.2d 686, 693 (2d Cir. 1992) (internal quotation marks and citation omitted).

2. Alleged Insufficiency of the Computer Intrusion Statutes

Defendant contends that the Indictment fails to allege several essential elements necessary to the Computer Intrusion Counts.[1] Specifically, Defendant argues that the Indictment fails to allege (1) that he accessed a "protected computer"; (2) that he gained "actual access" to

[1] Defendant's motion also states in passing that the Government fails to allege a prima facie case of wire fraud. (MTD at 3.) However, Defendant does not direct any of his arguments at the wire fraud charges, and the basis for his claim is unclear from the face of the Indictment. The court finds no reason to conclude that the Wire Fraud Counts are insufficiently pled and does not further address the point in this opinion.

information on those computers; (3) that he "obtained information" through the alleged unauthorized access; and (4) that Defendant derived any value from the intrusions. (See generally MTD at 3-6.) Before addressing these alleged insufficiencies, the court briefly reviews the statutes at issue in those counts and identifies the elements that the Government must allege in the Indictment. The court concludes that the Indictment contains sufficient allegations to survive a motion to dismiss.

a. The Computer Intrusion Statutes

i. 18 U.S.C. § 1030(a)(4) (Count One)

Section 1030(a)(4) states that:

> [Whoever] knowingly and with intent to defraud, accesses a protected computer without authorization . . . and by means of such conduct furthers the intended fraud and obtains anything of value [commits a crime], unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

18 U.S.C. § 1030(a)(4) (emphasis added). A "protected computer" is, inter alia, "a computer [] which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication." Id. § 1030(e)(2)(B). Courts have interpreted this definition to include "effectively all computers with Internet access." United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015) (quoting United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012)).

ii. 18 U.S.C § 1030(a)(2) (Count Two)

Section 1030(a)(2) makes it a crime to "intentionally access[] a computer without authorization . . . and thereby obtain . . . [i]nformation from any protected computer." 18 U.S.C. § 1030(a)(2). "Protected computer" here has the same meaning as that noted above.

b. Alleged Defects

i. Failure to Allege Access to a Protected Computer

Defendant claims that the Indictment fails to sufficiently allege that he accessed a "protected computer." (See MTD at 4-5.) As noted, however, the term "protected computer" encompasses "effectively all computers with Internet access."[2] Valle, 807 F.3d at 528 (internal quotation marks and citation omitted). The allegations that Defendant transmitted malware electronically in support of an online click fraud scheme necessarily involve internet-connected computers. (See Ind. ¶ 5-10.) Moreover, the Indictment's recitation of both Computer Intrusion Counts alleges that he accessed "one or more protected computers." (Id. ¶¶ 12, 14) Both separately and taken together, these allegations are sufficient to inform the Defendant of the charge against him with respect to that element. See Stavroulakis, 952 F.2d at 693 (stating that the "indictment must be read to include facts which are necessarily implied by the specific allegations made.")

Accordingly, the court denies Defendant's motion to dismiss based on the claimed failure to allege that he accessed a "protected computer."

ii. Failure to Allege "Actual" Access

Defendant maintains that the Indictment fails to allege that he had "actual access" to any U.S. servers, and at most alleges control of an automated botnet that provided the "capability to intrude into computers." (MTD at 3.) In connection with this argument, Defendant points to a statement in the affidavit submitted in support of his extradition that Defendant's "malicious

[2] At oral argument, Defendant argued that the term "protected computer" had been read overly broadly, pointing to the other, more specific prohibitions in Section 1030(a)(2) that apply to information obtained from financial institutions, credit card issuers, and federal agencies and departments. (Tr. of Hr'g on Mots. ("Hr'g Tr.") (Docket Number forthcoming) at 7-8.) However, given the breadth of the statutory language and other cases interpreting that language, the court sees no reason to adopt a different interpretation of "protected computer" than that provided above, nor does Defendant provide a suggested alternative definition.

software was found" in Queens-based law firm's server. (Id. at 4 (citing Extradition Aff. ¶ 9).) Defendant claims this allegation cannot support actual access because, at the time the malware was "found," Defendant was in custody. (See MTD at 4.)

Despite Defendant's contentions, however, the Indictment avers at several points that Defendant had actual access to computer servers, including access gained as part of the process of installing the malware. (See Ind. ¶¶ 6, 7, 12, 13.) These statements track the language of the statute and, combined with the approximate statements of dates and locations contained in the Indictment, are sufficient to withstand a motion to dismiss at this stage.

To the extent that Defendant's challenge is based on the Extradition Affidavit, that argument is not properly raised in a motion to dismiss. In weighing the validity of the Indictment, the court may not consider outside evidence. See, e.g., United States v. Foxworth, No. 3:06-CR-81 (AHN), 2006 WL 3462657, at *3 (D. Conn. Nov. 16, 2006); cf. also United States v. Brown, 321 F. Supp. 2d 598, 600 (S.D.N.Y. 2004) ("[I]t is axiomatic that . . . a defendant may not challenge a facially valid indictment prior to trial for insufficient evidence."). Further, it is not clear that the affidavit in fact supports Defendant's position, as it alleges that Defendant "gained entry into multiple servers." (Extradition Aff. ¶ 5.)

For these reasons, the court denies Defendant's motion to dismiss based on the claimed failure to allege "actual access" to computer systems.

iii. Failure to Allege that Defendant "Obtained Information" From a Protected Computer

Defendant argues that Count Two is insufficiently pled because the alleged scheme did not target "information" on protected computers. (See, e.g., Def. Reply Mem. ("Reply") (Dkt. 30) at 2-3.) Pointing to Section 1030(a)(2)'s requirement that a defendant obtain information from a protected computer though their unauthorized access, 18 U.S.C. § 1030(a)(2),

Defendant argues that "criminal liability is triggered . . . [only based on] actual obtainment of information that is itself needed—and not collateral—to carry out the fraudulent scheme" (Reply at 2). From this, he claims that the Indictment fails as a matter of law because the purpose of the alleged intrusion "was not the information that [the compromised computers] may or may not have contained, but rather the[ir] computing power." (Reply at 3.)

Whatever its merits, Defendant's argument is better considered at trial. The Indictment tracks the statute and alleges specifically that Defendant "obtain[ed] information from one or more protected computers" through his access to those computers. (Ind. ¶ 14.) Combined with other allegations specifying the approximate timeframe of Defendant's conduct, the Indictment satisfies the pleading threshold imposed by Rule 7. If Defendant is instead arguing that the Government cannot prove that he obtained information, he raises only an evidentiary issue that is insufficient to merit dismissal at this stage. See, e.g., United States v. Coffey, 361 F. Supp. 2d 102, 111 (E.D.N.Y. 2005) ("[T]he validity of an indictment is tested by its allegations, not by whether the Government can prove its case." (citations omitted)).

The court therefore denies Defendant's motion to dismiss based on the claimed failure to allege that he "obtained information."

iv. Failure to Properly Allege Value Lost as a Result of the Scheme Under Section 1030(a)(4)

Defendant's final argument is that the Government fails to establish that the losses from Defendant's alleged scheme totaled more than $5,000 per year, which he claims is required by Section 1030(a)(4). (MTD at 5-6.) Inherent in this argument is the underlying claim that the "object of the fraud and the thing obtained consists only of the use of the computer."[3] 18

[3] Defendant also argues that the Government is required to allege the value of the items obtained through the intrusion and cites several opinions from civil cases regarding Section 1030(a) claims. (See, e.g., Hr'g Tr. at 11-14.) Those opinions do not bear on a criminal prosecution, however. While Section 1030 permits civil actions by parties

U.S.C. § 1030(a)(4). (See also MTD at 5.) The Government responds that it is not obligated to allege a loss amount, as the Indictment alleges that he obtained "objects of value" other than the use of the compromised computers. (Mem. in Opp'n to MTD Mot. ("MTD Opp'n") (Dkt. 27) at 7.)

The Indictment's failure to allege the lost value attributable to the alleged intrusions does not undermine its validity. The plain language of the statute only requires the Government to establish the value of the loss as part of the violation if both the object of the fraud and the thing obtained are limited only to the "use of a computer." 18 U.S.C. § 1030(a)(4). The Indictment alleges that, through Defendant's intrusions, he obtained "information[] and United States and foreign currency" in addition to the "use of a computer." (Ind. ¶ 12).) Other allegations likewise indicate that the alleged fraud's purpose was merely to access computers but also to obtain revenue from the defrauded advertising companies. (Id. ¶ 9.) Crediting the Indictment's allegations, these claims are sufficient to support the charge against Defendant, and the Government is not required at this stage to claim any value attributable to the alleged intrusion.[4]

Accordingly, the court denies Defendant's motion to dismiss based on the claimed failure to allege the value lost as a result of the alleged scheme.

---

suffering loss or damage as a result of that section, the party bringing the action must allege that they have been harmed in one of five ways, including suffering more than $5,000 in aggregate losses over a one year period. See 18 U.S.C. § 1030(g). There is no such predicate imposed on criminal prosecutions, however. Id. § 1030(c).

[4] Defendant additionally argues that the losses alleged must have been suffered by the victim of the intrusion and not solely by a third party (see Reply at 4) and that the "statute is not designed to protect the financial interests of a foreign business" (MTD at 6). Defendant argues that losses suffered by the intended victim of the alleged fraud cannot be counted towards the value of the losses suffered by the alleged victims of the intrusions. (Id. at 4-5.) The court need not address this argument at this point, as the allegation that the objects of the fraud included more than use of the computers obviates the need for any allegation of value lost or gained.

3. *Extraterritoriality and Due Process Considerations*

Defendant makes two related arguments: first, that the Wire Fraud Counts cannot be applied extraterritorially as a general matter of statutory interpretation; and second, that neither the Wire Fraud nor the Computer Fraud Counts can be applied to him consistent with the Due Process clause of the Fifth Amendment.[5] (See MTD at 7-12.) The court finds that the Wire Fraud Counts do not require an extraterritorial application of the underlying statute, and that neither the Wire Fraud nor the Computer Fraud Counts violate Defendant's rights to due process. Accordingly, Defendant's motion to dismiss those counts is denied.

a. The Presumption Against Extraterritoriality

In support of his claim that the Wire Fraud Counts cannot be applied to conduct abroad, Defendant points to the presumption against extraterritoriality. (MTD at 11.) The presumption against extraterritoriality is a cannon of construction which states that "[a]bsent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." RJR Nabisco, Inc. v. European Cmty. ("RJR Nabisco II"), — U.S. —, 136 S. Ct. 2090, 2100 (2016) (internal citations omitted). Questions of extraterritoriality are assessed using a "two-step framework:"

> At the first step, we ask whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially. . . . If the statute is not extraterritorial, then at the second step we determine whether the case involves a domestic application of the statute . . . by looking to the statute's "focus." If the conduct relevant to the statute's "focus" occurred in the United States, then the case involves a permissible domestic application even if other conduct relevant to the focus occurred in a foreign country; but if the conduct relevant to the focus occurred in a foreign country, then the case

[5] Neither Defendant nor the Government addressed any statutory or due process concerns associated with the alleged money-laundering conspiracy, though Defendant stated at oral argument that he "would make an argument [regarding the money laundering statute] if the motion to dismiss is not granted." (See Hr'g Tr. at 44). Because the parties have not briefed the issue, the court does not address the money laundering count at this juncture.

> involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory.

Id. at 2101. Under the second step of this inquiry, courts looking for a statute's "focus" should identify "those transactions that the statute seeks to regulate." Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 267 (2010). Once determined, the court must look to the "territorial events or relationships" implicated by that focus, see Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 216 (2d Cir. 2016), and assess whether those events or relationships were located domestically or abroad under the facts before them. If the court finds that the contacts relevant to the focus in the case before it occurred domestically, then that application of the law is not impacted by the presumption against extraterritoriality. Id. ("If the domestic contacts presented by the case fall within the 'focus' of the statutory provision or are the 'objects of the statute's solicitude,' then the application of the provision is not unlawfully extraterritorial." (quoting Morrison, 561 U.S. at 267)).

b. Extraterritoriality of the Wire Fraud Counts

i. Applying the Two-Step Framework to the Wire Fraud Statute

In relevant part, the statute criminalizing wire fraud reads:

> Whoever, having devices or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses . . . transmits . . . by means of wire . . . in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or purpose [shall be deemed to have violated the law].

18 U.S.C. § 1343. The Second Circuit has determined that this language lacks clear indicia of intended extraterritorial application and so does not satisfy the first step of the analysis detailed above. See European Cmty. v. RJR Nabisco, Inc. ("RJR Nabisco I"), 764 F.3d 129, 140-41 (2d Cir. 2014), rev'd and remanded on other grounds, 136 S. Ct. 2090; see also United States v.

Hawitt, No. 15-CR-252 (PKC), 2017 WL 663542, at *4 (E.D.N.Y. Feb. 17, 2017) (applying RJR Nabisco I to a wire fraud prosecution). The panel expressly declined, however, to identify the "focus" of the wire fraud statute, finding instead that the Plaintiffs in that case "alleged [domestic] conduct . . . that satisfie[d] every essential element of the mail fraud . . . claims." RJR Nabisco I, 764 F.3d at 142 & n.14.

The limited number of opinions attempting to discern the "focus" of the wire fraud statute generally break into two camps: those emphasizing the "wires" and those looking to the "fraud." Courts in the first category have largely looked to the Supreme Court's decision in Pasquantino v. United States, 544 U.S. 349 (2005), as their source of authority. In that case, the Court briefly considered whether a wire fraud prosecution alleging a scheme to evade Canadian taxes constituted an impermissible extraterritorial application of that law and held that it did not. Id. at 371. Defendants were convicted of wire fraud based on their use of New York phone lines to order alcohol from another U.S. state, and that alcohol was then smuggled across the Canadian border. Id. at 353. The Court held that application of the wire fraud statute did not violate the prohibition on extraterritoriality, as the "offense was complete the moment [the defendants] executed the scheme inside the United States." Id. at 371. Several subsequent opinions have concluded that this holding dictates that any use of U.S. wires is sufficient to render application of wire fraud statute domestic. See, e.g., United States v. Hayes, 99 F. Supp. 3d 409, 421 (S.D.N.Y. 2015); United States v. Coffman, 771 F. Supp. 2d 735, 738-39 (E.D. Ky 2011).

On the other hand, several recent opinions reviewing the wire fraud statute and the substantially similar mail fraud statute found those statutes' "focus" was the "scheme to defraud." United States v. All Assets Held at Bank Julius, — F. Supp. 3d —, No. 04-CV-798, 2017 WL 1508608, at *15 (D.D.C. Apr. 17, 2017); United States v. Prevezon Holdings, Inc., 122

F. Supp. 3d 57, 71-72 (S.D.N.Y. 2015); see also Elsevier, Inc. v. Grossman, 199 F. Supp. 3d 768, 783-84 (S.D.N.Y. 2016) (concluding the mail fraud statute's focus is on the "particular class of frauds" prohibited in the statute). Drawing from this "focus," one court held that:

> a complaint alleges a domestic application of wire fraud when (1) a defendant or coconspirator commits a substantial amount of conduct in the United States, (2) the conduct is integral to the commission of the scheme to defraud, and (3) at least some of the conduct involves the use of U.S. wires in furtherance of the scheme to defraud.

Bank Julius, 2017 WL 1508608, at *15 (citing Elsevier, 199 F. Supp. 3d at 784).[6]

Considering these competing views, the court concludes that the wire fraud statute's "focus" is the fraudulent scheme. The court respectfully disagrees with the view that Pasquatino requires nothing more than U.S.-based wire transfers to demonstrate domestic application. Pasquantino considered only whether the fact that the ultimate victim of a fraudulent scheme rendered the application of the wire fraud statute impermissible extraterritorial, even though the underlying scheme was otherwise entirely carried out in the United States. Pasquantino, 544 U.S. at 371-72. The Court did not speak to the readily-distinguishable case of a scheme devised and otherwise executed abroad that involves some use of U.S. wires. Instead, the court agrees with the contrary opinion expressed above that Congress's focus in enacting the wire fraud prohibition was to regulate frauds, and not solely a means of perpetrating a fraud. Accordingly, the court analyzes the Indictment using the three-part test set forth in Bank Julius.

[6] While no decision separately addresses the extraterritorial application of the wire fraud conspiracy statute, other courts have concluded that "the extraterritorial reach of an ancillary offense like aiding and abetting or conspiracy is coterminous with that of the underlying criminal statute." United States v. Ali, 718 F.3d 929, 940 (D.C. Cir. 2013) (collecting cases). The court agrees that there is no reason to differentiate the extraterritoriality analysis as between "ancillary" offenses and the underlying substantive offense, and so the court's examination of the wire fraud violation applies equally to the related wire fraud conspiracy count.

ii. Application to the Wire Fraud Counts

Applying this tripartite test, the court concludes that the Wire Fraud Counts requires only domestic application of the underlying statutes, as the "click fraud" scheme was supported in large part by domestic conduct. While the face of the Indictment alleges only a single wire transfer (see Ind. ¶ 19), the Government represented to the court that it intends to present evidence that Defendant leased a server from a New Jersey-based company, which he used to make similar wire transfers in furtherance of the scheme to more than 800 compromised computers in the United States (see MTD Opp'n at 25; Hr'g Tr. at 42). Moreover, the Government provided further detail on the wire transfers themselves, describing how the "user agent string"[7] transfers allowed infected servers to "masquerade" as personal computers. (See Hr'g Tr. at 22-23.) This charade is vital to the alleged scheme, as it gives the victim advertising company the false impression that individual users are "clicking" on its advertisements. Considering both the large number of computers allegedly affected[8] and the importance of the wires to the fraud, the court concludes that the alleged domestic conduct related to the "click fraud" is both "substantial" and "integral to the commission" of the underlying scheme. See Bank Julius, 2017 WL 1508608, at *15.

Accordingly, the court denies the motion to dismiss the Wire Fraud counts based on the presumption against extraterritoriality. Defendant may, however, renew his objection to the

[7] A "user agent string" is a "file 'typically used by a software agent such as a web browser to identify itself . . . by submitting a characteristic identification string to its operating peer.'" (Combined Opp'n at 10 (quoting Compl. (Dkt. 1) ¶ 11 n.6).)

[8] Defendant argues that the court should view the number of servers in the context of the overall number of computers—upwards of 100,000 worldwide—allegedly infected by Defendant's malware. (Reply at 9.) This approach would, however, allow criminal defendants to dilute their responsibility in the United States by engaging in more criminal behavior in other countries. For this reason, the court concludes that the question of whether activity was "substantial" should be viewed objectively and not solely as a percentage of other activity in furtherance of the scheme.

Wire Fraud Counts on this basis at a later time once the Government provides further detail on the alleged domestic conduct in furtherance of the "click fraud" scheme.

4. Alleged Lack of "Nexus" to the United States

Defendant's final argument in favor of dismissal is that the Wire Fraud and Computer Intrusion counts violate his right to due process, as they fail to allege a "nexus" between the acts of which Defendant is accused and the United States. (MTD at 7-8.) In support of this argument, Defendants repeats many of his previous points, arguing that the Indictment fails to allege that he acted within the United States, intended to defraud any U.S. person or company, or obtained anything of value other than the use of U.S.-based computers.

Regardless of congressional intent, federal criminal statutes may only be applied extraterritorially where that application is consistent with due process requirements. United States v. Yousef, 327 F.3d 56, 86 (2d Cir. 2003). This requires showing a "sufficient nexus between the defendant and the United States, so that [extraterritorial] application would not be arbitrary or fundamentally unfair." United States v. Al Kassar, 660 F.3d 108, 118 (2d Cir. 2011) (internal quotation marks and citations omitted). "For non-citizens acting entirely abroad, a jurisdictional nexus exists when the aim of [the charged] activity is to cause harm inside the United States or to U.S. citizens or interests." Id. (internal citation omitted). Due process does not, however, require the defendant to be on notice that they would be "subject to criminal prosecution in the United States so long as they would reasonably understand that their conduct was criminal and would subject them to prosecution somewhere." Id. at 119.

The court finds that application of the charged counts to Defendant is consistent with due process. At the outset, the court notes that the Wire Fraud Counts are not subject to the due process limitations discussed above. As discussed in the preceding section, Defendant's alleged U.S.-based conduct renders application of the wire fraud statute to him domestic, and so he

cannot be said to have "act[ed] entirely abroad." Id. at 118. Moreover, to the extent that the Computer Intrusion Counts seek extraterritorial application of the underlying statute,[9] the acts alleged in those counts were "aim[ed] . . . [at] caus[ing] harm inside the U.S. or to U.S. citizens or interests," sufficient to satisfy due process. Id. at 118. The Indictment alleges that Defendant targeted U.S.-based computers for unauthorized access, compromise, and use in furtherance of the fraudulent scheme. (See, e.g., Ind. ¶¶ 6-7.) While Defendant argues that the ultimate aim of the alleged fraud targeted foreign companies and persons (see MTD Opp'n at 8), that larger aim does not negate the goal of the charged activity: targeting computers in the U.S. for intrusion and exploitation. This alleged purpose is sufficient to satisfy due process limitations on extraterritoriality.

Accordingly, the court concludes that application of the wire fraud and computer intrusion statutes here is consistent with due process and so denies Defendant's motion to dismiss the Indictment on that basis.

* * *

For the foregoing reasons, Defendant's motion to dismiss the indictment is denied in its entirety.

B. Motions for a Bill of Particulars and for Disclosure of Grand Jury Material

Defendant also seeks a bill of particulars and disclosure of grand jury information. Though governed by different standards, Defendant's motions raise substantially similar points.

---

[9] Unlike the wire fraud statute, the statute underlying the Computer Intrusion Counts has the indicia of congressional intent to apply extraterritorially. As noted, the statutory definition of "protected computers" includes computers that are "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). In adopting this definition of "protected computer," Congress was explicit in its purpose of ensuring that the law penalized "hackers" based outside of the United States, citing examples of foreign individuals who harmed United States computers. See S. Rep. No. 104-357, 1996 WL 492169, at *4 (1996). Viewed against this backdrop, Section 1030 is properly viewed as applying extraterritorially at least to prosecutions of foreign actors whose actions affect "protected computers" in the U.S. See United States v. Ivanov, 175 F. Supp. 2d 367, 374-75 (D. Conn. 2001); cf. also Microsoft, 829 F.3d at 219-20 (relying in part on legislative history to determine a statute's "focus").

First, Defendant argues that the allegation that he "obtained information" through the alleged computer intrusions (Ind. ¶ 14) is inconsistent with the alleged "click fraud" scheme. (See BOP Mot. at 1; GJ Mot. at 1-2.) Second, Defendant contends that there is no support for the alleged connection between the Eastern District of New York and himself, his co-conspirators, or the acts committed in furtherance of the conspiracy. (See BOP Mot. at 2; GJ Mot. at 2-3.)

For the reasons that follow, the court grants in part and denies in part Defendant's motion for a bill of particulars and denies Defendant's motion to unseal grand jury materials.

1. Motion for a Bill of Particulars

In his motion for a bill of particulars, Defendant seeks additional specification regarding (1) the alleged computer intrusions; (2) the conspiracy; (3) the transactions at issue in the money-laundering counts; and (4) the allegedly fraudulent wire transfers and underlying scheme.[10] (See BOP Mot. at 3-4.) In response, the Government argues that Defendant has not shown a need for the requested information and that it has already "disclos[ed] [] nearly all of the requested facts," through the Complaint, Indictment, and discovery.[11] After review of the parties' submissions, the court orders the Government to provide limited additional information regarding the alleged computer intrusions but denies the remaining requests.

a. Legal Standard

The purpose of a bill of particulars is to allow a defendant "to identify with sufficient particularity the nature of the charge pending against him, thereby enabling a defendant to

[10] Defendant also requests a bill of particulars stating whether he is alleged to have participated as a principal or an aider and abettor with regard to each charged count. (See BOP Mot. at 3-4.) In its opposition to the motion, however, Government explicitly states the method of liability charged with respect to each count, mooting that request. (See Mem. in Opp'n to BOP & GJ Mots. ("Combined Opp'n") (Dkt. 39) at 7.)

[11] The Government also argues that Defendant fails to provide "good cause" to support his filing of the motion for a bill of particulars outside of the 14 day window set by Federal Rule of Criminal Procedure 7(f). (Combined Opp'n at 3.) However, the court previously granted Defendant leave to file the motion (May 18, 2017, Min. Entry), and so this argument is not discussed here.

prepare for trial, prevent surprise, and to interpose a plea of double jeopardy." United States v. Bortnovsky, 820 F.2d 572, 574 (2d Cir. 1987). Decisions as to whether or not to grant a bill of particulars are left to "the sound discretion of the district court." United States v. Davidoff, 845 F.2d 1151, 1154 (2d Cir. 1988). Courts are only required to grant a bill of particulars where the charges of the indictment are so general that they do not "advise the defendant of the specific acts of which he is accused." United States v. Chen, 378 F.3d 151, 163 (2d Cir. 2004) (internal quotation marks and citation omitted). Whether this standard is met turns on "whether the information sought is necessary, not whether it is helpful." United States v. Facciolo, 753 F. Supp. 449, 451 (S.D.N.Y. 1990). In making this determination, "the court must examine the totality of the information [already] available to the defendant—through the indictment, affirmations, and general pre-trial discovery." United States v. Bin Laden, 92 F. Supp. 2d 225, 233 (S.D.N.Y. 2000); see also Bortnovsky, 820 F.2d at 574 ("Generally, if the information sought by the defendant is provided in the indictment or in some acceptable alternate form, no bill of particulars is required.").

b. Application to the Categories of Information Sought by Defendant

i. Information Concerning the Alleged Computer Intrusions

Defendant requests specification of both the dates and times of the alleged access to protected computers and the nature and location of the information allegedly obtained as a result of that unauthorized access. (BOP Mot. at 3.) The Government contends that it has provided much of this information through document discovery and early disclosure of expert witness reports, including disclosure of the "manner in which [the malware] infects targeted computers and . . . operates once inside the computers" and the Internet Protocol ("IP") addresses and locations of infected computers. (See Mem. in Opp'n to BOP & GJ Mots. ("Combined Opp'n") (Dkt. 39) at 8-9; Hr'g Tr. at 40-41, 43.)

Despite the insight provided by the Government's existing productions, the court concludes that there remains a risk of unfair surprise that must be mitigated. On the one hand, the categories of material already provided by the Government, particularly the compromised servers' IPs and location information, offer sufficient guidance regarding Defendant's alleged access to those servers. While that information does not directly identify the date and time of Defendant's alleged access, it is sufficient to refine his review of other discovery materials and ensure that he has a fair opportunity to prepare for trial. However, as discussed above, the Indictment alleges that Defendant "obtained information" through his unauthorized access to a protected computer (Ind. ¶¶ 12, 14), but does not elaborate on this claim. Defendant argues persuasively that the information that could be obtained through the "click fraud" scheme is not obvious from the existing allegations. Moreover, Defendant cannot look to other, similar prosecutions for guidance as to this element, as this is a "cutting-edge" case by the Government's own admission. (Hr'g Tr. at 21.) Despite the suggestion that insight into the information allegedly obtained may be gleaned from the Government's expert report disclosures (see Hr'g Tr. at 20-21; Combined Opp'n at 8-9), the court is concerned that, in this unique prosecution, Defendant is effectively unguided as to one of the elements of the Computer Intrusion Counts[12] and so is impaired in his ability to prepare for trial.

Accordingly, the court orders the Government to provide a bill of particulars identifying the categories of information allegedly obtained in connection with the Computer Intrusion Counts.

[12] While Count One, alleging a violation of Section 1030(a)(4), does not necessarily require the Government to prove that a defendant "obtained information," it does require a showing that he or she obtained "anything of value." 18 U.S.C. § 1030(a)(4). Here, the Government alleges that one of the things of value obtained as a result of the intrusion was "information," (Ind. ¶ 12) and so incorporates that "information" into its recitation of the elements.

ii. Conspiracy and Co-Conspirator Information

Defendant seeks several categories of information relating to the conspiracy, including identification of his alleged co-conspirators, the date, time, and location of the conspiracy's initiation, and the overt acts perpetrated in furtherance of the conspiracy charges.[13] (See BOP Mot. 3-4.) In response, the Government points to productions which purportedly provide much of the information requested, including records of payments made to Defendant and other co-conspirators, records associated with the websites maintained by Defendant and his alleged co-conspirators, and payments and communications between the alleged co-conspirators. (Combined Opp'n at 6-7.)

Criminal defendants are not automatically entitled to identification of unindicted co-conspirators. United States v. Follieri, No. 08-CR-850 (JGK), 2009 WL 529544, at *1 (S.D.N.Y. Mar. 3, 2009) (collecting cases). Courts considering requests for co-conspirator identification consider factors including:

> (i) the number of co-conspirators; (ii) the duration and breadth of the alleged conspiracy; (iii) whether the Government otherwise has provided adequate notice of the particulars; (iv) the volume of pre-trial discovery; (v) the potential danger to co-conspirators and the nature of the alleged criminal conduct; and (vi) the potential harm to the Government investigation.

United States v. Nachamie, 91 F. Supp. 2d 565, 572 (S.D.N.Y. 2000). Other details of a conspiracy, including requests for "the nature of the 'wheres, whens, and with whoms'" of a conspiracy, are frequently "held to be beyond the scope of a bill of particulars." United States v. Barret, 824 F. Supp. 2d 419, 439 (E.D.N.Y. 2011) (internal citation omitted) (collecting cases).

[13] Defendant's requests appear to be directed at understanding the basis for the allegation that he and others conspired "within the Eastern District of New York." (See BOP Mot. at 2.) At oral argument, however, the Government clarified that it does not allege that Defendant or his alleged co-conspirators were located in the United States but only that they engaged in conduct in the United States, such as infecting U.S.-based computers with malware and engaging a New Jersey company to host a server for the alleged scheme. (Hr'g Tr. at 45.)

Similarly, "[t]here is no general requirement that the government disclose in a bill of particulars all the overt acts it will prove in establishing a conspiracy charge." United States v. Carroll, 510 F.2d 507, 508-09 (2d Cir. 1975).

The court concludes that the Government's disclosures to date adequately inform Defendant of the information sought through these requests. Many of the factors listed above might, in other circumstances, weigh in favor requiring disclosure of the co-conspirators' identities. However, the information already provided by the Government includes explicit listing of the Defendant's brother as a co-conspirator in the Complaint as well as email and payment records identifying the other alleged co-conspirators by name. (Combined Opp'n at 6-7.) These disclosures obviate the need to further identify those individuals through a bill of particulars. Moreover, Defendant's requests for the overt acts, location, dates, and duration of the conspiracy go beyond the scope of the information to which he is entitled, as they seek the "wheres, whens, and with whoms" of the conspiracy. Barret, 824 F. Supp. 2d at 439; see also United States v. Walker, 922 F. Supp. 732, 739 (N.D.N.Y. 1996) ("[D]etailed evidence of a conspiracy is generally unavailable to defendants through a bill of particulars, and overt acts in furtherance of the conspiracy need not be disclosed.").

For these reasons, the court denies Defendant's request for a bill of particulars specifying additional information regarding the conspiracy and co-conspirators.

iii. Information Regarding the Money-Laundering Conspiracy

Defendant seeks additional information regarding the financial transactions alleged to be part of the money-laundering scheme, and also the "nature, location, source, ownership and control of the proceeds" allegedly laundered. (BOP Mot. at 4.)

The court finds that no bill of particulars is required in light of the existing disclosures. The Government's statement that it has already provided Defendant with the transactions alleged

to constitute money laundering averts the need for a bill of particulars in that regard. Moreover, Defendant's further request for specification of the source of the proceeds is not necessary to understand the charges against him. The Indictment specifies that the purpose of the alleged laundering transactions was to conceal the proceeds of the alleged computer intrusions and wire fraud. (See Ind. ¶ 21.) This limitation appropriately cabins the scope of Defendant's trial preparation and removes the risk of unfair surprise. Cf., e.g., United States v. Stern, No. 03-CR-81 (MBM), 2003 WL 22743897, at *4 (S.D.N.Y. Nov. 20, 2003) (concluding that identification of the wrongful conduct the defendant sought to conceal was necessary to avoid unfair surprise).

Accordingly, the court denies Defendant's motion for a bill of particulars providing further details of the money laundering transactions at issue.

iv. Information Regarding the Wire Fraud

Defendant's final request seeks further information regarding the alleged fraudulent scheme underlying the Wire Fraud Counts. He specifically seeks the time and location of any fraudulent misrepresentations, and the recipients of the "user agent string" that was allegedly transmitted to compromised computers by use of the wires. (See BOP Mot. at 3.)

The court again concludes that existing disclosures by the Government adequately apprise him of the basis for the charges against him. The Government represented that it has provided IP addresses and locations of the 800 computers alleged to have been affected by the malware (Hr'g Tr. at 40), a disclosure which directly answers Defendant's request for information about the recipients of the "user agent string." Further, while the Government has not disclosed the specific times and locations of any fraudulent misrepresentations, Defendant is also apprised of the nature of the alleged misrepresentations through the description of the alleged "click fraud" scheme through the Indictment, the Complaint, and other filings. Combined with the Government's production of payments by the advertising companies

allegedly targeted in that scheme (Combined Opp'n at 6, 11), these descriptions provide Defendant with sufficient information to understand the charges against him, prepare his defense, and avoid unfair surprise at trial.

Accordingly, the court denies Defendant's request for a bill of particulars providing additional information detailing the misrepresentations and wire transmissions underlying the alleged wire fraud.

2. Motion for Disclosure of Grand Jury Material

Defendant moves for an order requiring disclosure of the colloquy to and testimony given before the grand jury that indicted him. Defendant claims that this information is necessary to "support his motion to dismiss and/or cross-examine Government witnesses." (See GJ Mot. at 1.) In support of his motion, Defendant reiterates his need for further information regarding the allegations that he "obtained information" from protected computers and that he entered into a conspiracy that "took place within the Eastern District of New York." (See GJ Mot. at 1-3.) Defendant argues that the grand jury minutes may provide insight into the basis for these allegations, explicitly suggesting that they may have resulted from misrepresentations or omissions by the prosecutor. (Reply in Supp. of GJ Mot. ("GJ Reply") (Dkt. 41) at 2-3; see also Hr'g Tr. at 47-48.)

a. Legal Standard

Rule 6 of the Federal Rules of Criminal Procedure permits courts to "authorize disclosure—at a time, in a manner, and subject to any other conditions that it directs—of grand-jury matter . . . at the request of a defendant who shows that a ground may exist to dismiss the indictment because of a matter that occurred before the grand jury."[14] Fed. R. Civ.

[14] Defendant initially framed his motion as falling under Rule 6(e)(3)(E)(i), which permits disclosure of grand jury material "preliminarily to or in connection with a judicial proceeding." (GJ Mot. at 1.) However, Defendant's

P. 6(e)(3)(E)(ii). Decisions as to whether disclosure is warranted based on those considerations are left to the court's discretion. See In re Petition of Craig, 131 F.3d 99, 104 (2d Cir. 1997).

"[T]he party seeking disclosure [of grand jury materials] must show a 'particularized need' that outweighs the need for secrecy." United States v. Moten, 582 F.2d 654, 662 (2d Cir. 1978). "[R]eview of grand jury minutes is rarely permitted without specific factual allegations of government misconduct." United States v. Torres, 901 F.2d 205, 233 (2d Cir. 1990) (abrogated on other grounds). Defendants do not meet this standard where they "offer little more than speculation that some impropriety may have occurred before the grand jury." United States v. Ordaz-Gallardo, 520 F. Supp. 2d 516, 519 (S.D.N.Y. 2007). Moreover, challenges cannot be based allegations that a grand jury returned a "facially valid indictment" based on "inadequate or incompetent evidence." United States v. Calandra, 414 U.S. 338, 345 (1974); see also United States v. Dunn, No. 05-CR-127 (KMK), 2005 WL 1705303, at *2 (S.D.N.Y. July 19, 2005) (applying Calandra to a motion under Rule 6(e)(3)(E)(ii)).

b. Application

Defendant fails to satisfy the burden of particularized need necessary to obtain review of grand jury materials. At root, Defendant's arguments are based on speculation that the grand jury could not have been convinced to return the charges against him based on the evidence he has reviewed. For instance, he argues that the fact that neither he nor his alleged co-conspirators were alleged to be in New York as incongruous with the allegation that the conspiracy "took place 'in the Eastern District of New York.'" (GJ Mot. at 2.) From this, he conjectures that the

---

motion is based explicitly on his contention that "material misrepresentation of facts as well as crucial omissions may have been made during the proceedings leading to the indictment." (Reply in Supp. of GJ Mot. ("GJ Reply") (Dkt. 41) at 1; Hr'g Tr. at 43.) Accordingly, the court treats Defendant's motion as seeking disclosure based on alleged prosecutorial misconduct before the grand jury and addresses it under the more appropriate standard quoted above.

prosecutor must have provided incomplete disclosures or made material misrepresentations to the grand jury.[15] This speculation is not grounded in any "specific factual allegations," however, and does not merit unsealing that information. Torres, 901 F.2d at 233.

Accordingly, the court denies Defendant's motion to unseal material from the grand jury that indicted him.

III. CONCLUSION

For the foregoing reasons, Defendant's motions to dismiss the indictment and for disclosure of grand jury materials are DENIED WITHOUT PREJUDICE, and his motion for a bill of particulars is GRANTED IN PART and DENIED IN PART. The Government is ORDERED to provide Defendant with a bill of particulars identifying the categories of information alleged to have been "obtained" in connection with the Counts One and Two of the Indictment by no later than June 9, 2017.

SO ORDERED.

s/Nicholas G. Garaufis

Dated: Brooklyn, New York
May 31, 2017

NICHOLAS G. GARAUFIS
United States District Judge

[15] When asked about this point at oral argument, the Government clarified that it alleges only that "there was a significant amount of conduct integral to the scheme which took place [in the United States,] including hundreds of computers that were affected and infected by the malware." (See Hr'g Tr. at 45.)